# RFID

## Applications, Security, and Privacy

AIM Global, Inc.
CASPIAN
Center for Democracy and Technology
EPCglobal, Inc.
The Galecia Group
Gemplus
Institute for the Future
Matrics, Inc.
MIT Computer Science & Artificial Intelligence Laboratory
MIT Media Laboratory
OATSystems
Privacy Journal
The Privacy Rights Clearinghouse
The Procter & Gamble Company
RSA Laboratories
UCLA Department of Geography
Wayne State University Law School

EDITED BY
SIMSON GARFINKEL · BETH ROSENBERG

# RFID

## Applications, Security, and Privacy

Edited by
**Simson Garfinkel**
**Beth Rosenberg**



Addison-Wesley

Upper Saddle River, NJ • Boston • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

*Library of Congress Cataloging-in-Publication Data*
Garfinkel, Simson.
RFID : applications, security, and privacy / Simson Garfinkel and Beth Rosenberg, editors.
p. cm.
Includes index.
ISBN 0-321-29096-8 (alk. paper)
1. Inventory control—Automation. 2. Radio frequency identification systems. 3. Privacy, Right of—United States. I. Rosenberg, Beth II. Title.
TS160.G37 2005
658.5'14—dc22

2005006610



ISBN 0-321-29096-8
Text printed in the United States on recycled paper at Courier in Westford, Massachusetts.
First printing, July 2005

# RFID

# FOREWORD

Radio frequency identification (RFID) is the first important technology of the twenty-first century. That's an awesome responsibility. The first important technology of the twentieth century, radio, had a profound impact: Its descendents included television, computers, and even air travel. Big, fundamental technologies do that—they are the first steps onto a new continent of possibility. What follows are decades of exploration and discovery, much of it entirely unexpected and initially unbelievable.

RFID is important because it enables machines to perceive. Machine perception is common in science fiction, where sentient robots walk and talk as a matter of course, but it is rare and primitive in everyday life. Airport faucets struggle to sense people impatiently waiting to wash their hands, bar code scanners frequently fail to beep, and home burglar alarms have trouble distinguishing between pets and intruders. During the next few decades, RFID will help change all that: It will usher in a new wave of computing in which devices can effectively sense and interpret the world around them.

RFID, as its name suggests, is the means of identification. Later, related technologies will piggyback on RFID infrastructure to provide data about things like temperature, pressure, and wear. Warehouses will sense whether they are low on stock or overstocked; airports will find and route luggage automatically; cars will know whether their tires are about to blow; homes will know if lights are left on, doors are unlocked, or windows are open. Because of RFID, we are entering what Paul Saffo has called "The Sensor Age." In the nineteenth century, machines could do; in the twentieth century, they could think; in the twenty-first century, they will perceive.

For some, this is a Utopian vision. For others, it sounds like hell. As usual, the reality will be somewhere in between. To dispense with Utopia first: One thing is certain about the future—it won't ever be perfect. RFID will not cure war, end hunger, or eliminate all waste. But it may help sustain our world, increase our standard of living, raise the efficiency of our economy, and enhance the quality of our lives. At its very best, it may improve healthcare by making

pharmaceutical distribution more efficient and accurate; it may lead to more recycling by providing automatic sorting of garbage; and by improving the efficiency of government and business alike, it could contribute to lower prices and, maybe, reduced taxes. These are real benefits, of real value both to individual lives and to the human race as a whole. And this is just what we see today; there will be other benefits too, as yet unimagined. The technologies of the twentieth century—television, radio, computing, and so on—brought comparable advantages. Major technologies often start out as luxuries, indulgences, or conveniences and then, because they reshape society, become essential.

On the other side of the debate are those who think RFID means instant doom. Another certainty is that the world will not end in our lifetime. (Noam Chomsky jokes that this is the safest prediction to make because if you are wrong, no one will be around to notice.) All new technologies merit diligence. RFID is no different. Its risks must be measured, and where appropriate, we should be cautious. But not all risks are equal, and some must be dismissed to improve the debate.

First, RFID is not the work of the Devil. The Devil, by all accounts, is a supernatural being with inhuman powers: He doesn't need RFID. Second, RFID is not part of a plot by evil corporate interests intent on spying on everyone. A corporation, in contrast to the Devil, is a group of human beings with human powers, not evil villains who conspire against their customers. The people who work at corporations are interested in RFID because they think it will help them build a better business, not because they are secretly out to get us. Third, RFID is not about to give rise to a whole new class of totalitarianism. While dictators and oppressors *are* out to get us—or at least some of us—they have regrettably managed very well over the centuries without RFID. Dictators will use whatever they can to work their evil, but whether or not they succeed in the future probably has little to do with new technology.

Once these dramatic exaggerations are excluded, we are left with some important, serious, and reasonable questions. How can we know when and how RFID is being used? How can we make sure it is not misused? How can we exercise choice over how it affects us personally? How do we ensure that it is safe?

This book is an important contribution to the ongoing effort to find the answers. My friend and colleague, Sanjay Sarma, says, "Writing is the highest form of thought." It follows that reading allows us to hold other people's thoughts up to the light for closer examination. We can test their logic, measure their assumptions, and check their sources. Written argument has a vulnerability that is not found in sound bites, speeches, or journalism where it is too easy to gloss and gild and misrepresent. A written idea is a naked idea.

I do not agree with everything that is written here, but I welcome every word. RFID is too important for there to be no public debate or for a debate that is badly informed, sensationalized, or manipulated. It is an inevitable technology, and its impact will be felt for generations. We are at the start of a new century, the beginning of our adventure in machine perception, and the dawning of the Sensor Age. Now is the perfect time to wonder.

*—Kevin Ashton*
*cofounder and former executive director, Auto-ID Center*
*vice president, ThingMagic Corporation*
*February 2005*

# PREFACE

There's a school bus stopped outside a middle school in Spring, Texas, a wealthy suburb on the northern edge of Houston's metropolitan sprawl. Inside the bus, several well dressed and obviously well-off children stand in the aisle waiting to get off. Sandra Martinez, a 10-year-old with a thick brown braid and a charcoal gray blazer, pauses while she takes her ID card, hanging from a lanyard around her neck, and presses it against the large gray panel mounted on the big padded barrier that divides the stairwell from the passenger compartment.

The panel beeps.

Sandra descends the school bus steps and the next student fumbles for her ID card. Meanwhile, a computer onboard the bus is hard at work. First the computer takes a geospatial reading from the Global Positioning System receiver that's mounted inside the bus. Next, the computer, using an onboard digital cell phone, sends to Spring Independent School District the precise time and location that Martinez left the bus. This information is made instantly available on a Web site where it can be accessed by Martinez's parents, the school administration, or anyone else with the appropriate access codes. The purpose of the system, which was installed at a cost of $180,000, is to let parents know precisely when and where their children get on or off the school bus. "If it works one time, finding a student who has been kidnapped, then the system has paid for itself," Brian Weisinger, the head of transportation for the Spring district, told the *New York Times.*[1]

No student has ever been kidnapped in Spring, Texas.

1. Richtel, M. "In Texas, 28,000 Students Test an Electronic Eye." *The New York Times.* November 17, 2004. p. A1.

A slightly different student tracking system is in use at the Enterprise Charter School in Buffalo, New York. There, a pair of kiosks that were purchased at a cost of $40,000 read ID tags as students enter and exit the building. Mark Walter, head of technology for the Buffalo school, told the *New York Times* that initially, the system failed to register some students, but now it works pretty well. Advocates of the technology say that it just might be expanded—for example, with readers placed on individual classroom doors to see if students are attending their classes.

Some students, of course, invariably forget their tags at home or lose them. Some might even purposely throw them away. Even for these students, technology has an answer: In late 2004, the U.S. Food and Drug Administration approved for general use a tiny radio tag that can be implanted under the skin. Similar technology has been used to track household pets since the 1990s.

Meanwhile, the U.S. State Department is discussing the prospect of issuing passports that carry a tiny RFID chip that includes 64 kilobytes of memory and alas can be covertly read at a distance of 30 feet by anyone with a suitable reader and a good antenna.[2] The State Department says that there's no need to worry: The data on the chip will reportedly be encrypted, so anybody who reads it will read only gibberish.

## The RFID Controversy and the Technology That Fuels It

Radio Frequency Identification, better known as RFID, is fast becoming one of the most controversial technologies of our era.

Proponents of RFID say that the tiny tags, made of silicon chips and radio antennas, can stamp out counterfeit drugs, fight terrorism, and at the same time help Wal-Mart keep its shelves stocked. They say that widespread adoption of RFID will allow companies to improve efficiency, cut costs, and offer dramatic new products and services to their customers. Most proponents scoff that the technology has a downside at all—other than perhaps the cost of the tags, and the cost of tags is dropping quickly.

But RFID has many critics. The most vocal are privacy activists who argue that the technology's unprecedented ability to track the movements of individually

2. Wald, M.L. "New High-Tech Passports Raise Snooping Concerns." *The New York Times*. November 26, 2004.

serialized objects could be turned around and used to track the people carrying those objects. They worry that the RFID readers across the nation could report back to a single global network that could be used by the government as a kind of roving geographical wiretap.

Many critics argue that RFID is a threat not just to individuals but to corporations and governments as well. In a few years, RFID readers at warehouse doors will allow companies to inventory the contents of cartons without opening them. But without the proper controls, the technology could also facilitate industrial espionage by giving competitors unprecedented access to a company's inventory. And once you begin thinking about RFID as an offensive technology, a lot of possibilities start emerging. Just as toll roads can use RFID to read E-ZPass tags and automatically debit drivers' accounts, a bomb with a built-in RFID reader could wait patiently in the roadway until it senses the tag of a particular individual drives above, and then detonate. Want to falsely implicate someone in a crime? Just clone one of that person's RFID tags and then arrange for it to pass by a particular reader just minutes before a murder.

The book you are holding is the first of its kind to explore the wide range of security and privacy issues that are being raised by RFID technology. It is the first book to bring together advocates and opponents from across the RFID spectrum. In its pages you will find chapters from companies that are producing RFID readers; from companies that are busy putting products with embedded RFID-tags on their shelves; and from the very privacy activists who are trying to stop them. Bringing together this diverse group of individuals and organizations has taken a lot of time and work. The result is the most balanced and accurate discussion you will find of RFID technology and its attendant controversy anywhere on the planet.

## RFID: What Is It?

As its name implies, the term RFID is generally used to describe any technology that uses radio signals to identify specific objects. In practice, this means any technology that transmits specific identifying numbers using radio. Electronic Article Surveillance (EAS) systems, used by many clothing and music stores to set off an alarm when a shoplifter steals an item, are not RFID because the EAS tags do not have individual codes or serial numbers that can be read remotely. The Mobil Speedpass system used to pay for gas *is* an RFID system: Each Speedpass tag contains a unique serial number that is used to identify the tag's owner.

Each RFID tag consists of a silicon chip, an antenna, and some kind of housing. The tags come in sizes as large as a paperback book and smaller than a grain of

rice. So-called active tags contain batteries, while passive tags are powered directly by the radio frequencies used to read them. The reading range of a tag depends on many factors, including on the tag's electronics, its antenna, the reader, the radio frequencies used, and decisions made at the time the system is deployed. It is therefore inaccurate to state a "typical tag's" read range without first specifying what kind of tag you are using. (I explain these technical issues and others in Chapter 2, Understanding RFID Technology.)

Already, RFID technology is broadly deployed within the United States. Between the "proximity cards" used to unlock many office doors and the automobile "immobilizer chips" built into many modern car keys, it's estimated that roughly 40 million Americans carry some form of RFID device in their pocket every day. I have two: Last year MIT started putting RFID chips into the school's identity cards, and there is a Philips immobilizer chip inside the black case of my Honda Pilot car keys. Don't think you have an immobilizer chip? Look at Figure 1—you might be surprised.

Many of today's media accounts of RFID aren't about these proprietary devices or RFID in general but about the standardized Electronic Product Code (EPC) chips that were developed by the Auto-ID Center and are now being overseen

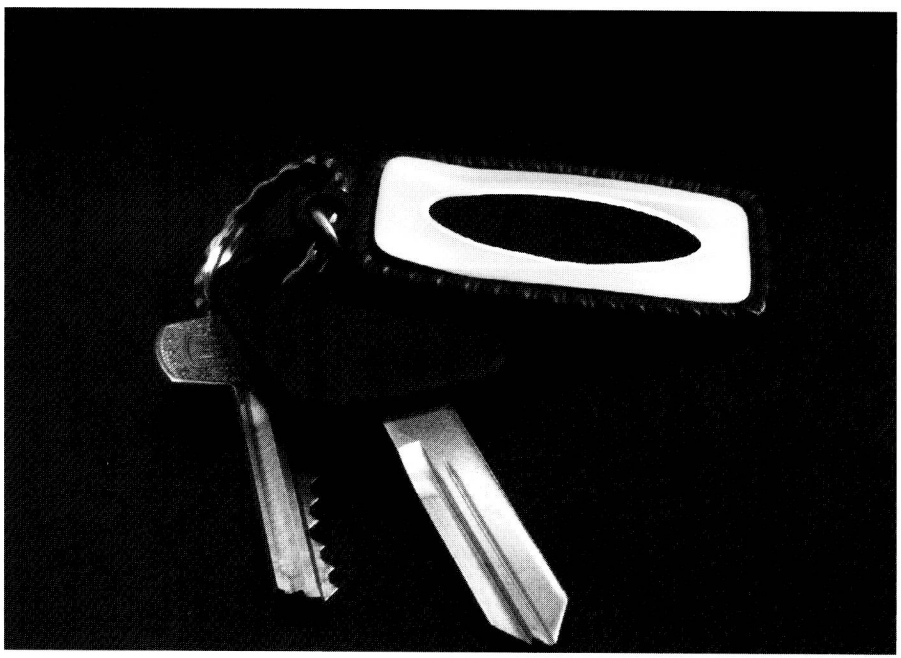

**Figure 1** The Immobilizer is built into the housing of the auto key. (Image reprinted courtesy of Texas Instruments Inc.)

by EPCglobal, a trade organization. RFID systems have been around for more than thirty years, opening office doors and tagging laboratory animals, but when the EPC was introduced, these systems were too expensive for mass deployment. By standardizing on a simple chip design and over-the-air protocol, EPC is able to take advantage of mass production's efficiencies.

EPC tags are designed to replace today's ubiquitous Universal Product Code (UPC) bar codes, except instead of identifying the maker and kind of product, the 96-bit EPC code will give every package of razors, box of pancake mix, and pair of sneakers its own unique serial number. The tags, which operate in the unlicensed radio spectrum between 868MHz and 965MHz, can be read at a distance of many feet and through paper, fabric, and some plastics. And although the tags can cost as much as 40 cents today, when they are purchased by the millions, the cost rapidly decreases to 10 cents per tag or less. (Sanjay Sarma, one of the founders of the Auto-ID center, explains the birth of the Auto-ID center and the EPC in Chapter 3, A History of the EPC.)

## RFID Comes of Age

I had my first experience with RFID technology in January 1984. I was a freshman at the Massachusetts Institute of Technology and had just taken a job at one of MIT's new biology labs. For added security, the lab had installed a keyless entry system. The lab gave me a thick blue card to put in my wallet. To get into the secure area, all I had to do was wave my wallet in front of a special reader. Within a few days I learned that I could just bump against the reader, leaving my wallet in my pocket. It was very cool and high tech and allegedly very secure.

After a few weeks in my wallet, the top layer of the card's plastic was starting to peel away. And a few days after I quit that job, I ripped open the card to see how it worked. Underneath the laminate, I found a printed circuit board, a chip that was the size of a postage stamp, and a dozen or so metal pads, some of them shorted together with a dab of solder.

It was immediately clear that my card's serial number was determined by which pads were soldered together and which had been left open. My ID number had been canceled when I resigned, but in theory I could have changed my card's ID to someone else's simply by making or breaking a few connections on the card. I never tested this hypothesis, but there is no reason it shouldn't have worked. (Twenty years later, the security of many proximity card systems has only marginally improved; Jonathan Westhues explores other ways of subverting the security of proximity cards in Chapter 19, Hacking the Prox Card.)

I promptly forgot about RFID for the next ten years. Then, in 1994, my editor at *Wired Magazine* asked me to write a brief article about ID chips that were being injected into cats and dogs. I called the chip manufacturer and learned that the technology was being used for far more. Some firms were using RFID to track the movement of gas cylinders; other companies were using it to follow the paths of tools at job sites. A few nursing homes were even experimenting with tagged bracelets that could automatically set off alarms when Alzheimer patients wandered out the back door.

A few months later I learned that highway authorities from Massachusetts and New York to California were in the final stages of testing RFID-based Electronic Toll Collection (ETC) systems for a variety of highways and bridges. The tags, which could be read at speeds of 100 miles per hour, would cut traffic jams and the resulting levels of smog at toll booths. But it was also clear that the new ETC systems would create a huge database recording the precise time and location of every toll crossing by every tagged car.

The planners of those early RFID systems said that it was important to establish policies that would prevent toll-crossing information from being used for purposes unrelated to traffic management. But such policies were never adopted. These days ETC databases are routinely used by law enforcement agencies to track the movement of suspect cars—and by both divorce lawyers and labor lawyers to track the movements of people under investigation. I spoke with these technologists in the 1990s: None of them wanted to create a ubiquitous surveillance system that would permanently record the movements of cars on the highways and make that information available to anybody with a subpoena. Yet somehow, that's the system we got.

Newspaper and magazine stories about RFID frequently present the technology as one that forces us to make tradeoffs and compromises. Almost always, RFID is portrayed as promising some new convenience or security feature, but in return, consumers must be willing to give up a little privacy to reap these benefits.

ETC is perhaps the best example of this tradeoff. With an E-ZPass tag, you can speed through the toll booths on the George Washington Bridge, but that nasty divorce attorney will be able to get a blow-by-blow record of every time you entered and left Manhattan for the past year.

But making E-ZPass a combination toll payment and surveillance system was a conscious choice on the part of the engineers who designed the system and the highway administrators who approved it. Instead of broadcasting a serial number that's used to debit an account, the creators of E-ZPass could have adopted a more complex over-the-air protocol based on anonymous digital cash. Such a

system would actually have been more secure—that is, more resistant to various kinds of cloning, fraud and abuse—than the account-based systems in a growing number of states. But as near as I have been able to determine, the system based on digital cash was never seriously considered.

The question of whether or not the nation's ETC system should preserve privacy or be a tool of surveillance should have been a subject of public debate. But it wasn't. Instead, policy was determined by a small number of technologists and administrators with virtually no input from either the public or elected officials.

In Massachusetts, for instance, when the Massachusetts Turnpike Authority (MTA) issued its request for proposal to contractors interested in supplying the ETC technology to the state, the RFP mandated that respondents propose only account-based systems similar to New York's E-ZPass. (Not surprisingly, a Boston-area company called ATCom, which had a system based on anonymous digital cash, cried foul, arguing that it had been frozen out of the bidding process because it had a technology that preserved privacy!)

John Judge was the MTA official responsible for the decision. When I called him to ask about the RFP, he told me in 1997, "Privacy is a non-issue."

> I think that is the experience nationwide, as least as it relates to electronic toll collection. Privacy has not been an issue that has emerged nationally. I think that [is] principally because it is a voluntary system. If you are of a mind where you might be concerned about privacy issues, you just don't have to join the program, and can use the traditional toll collection methods. I don't think that it is any more an issue than credit cards.[3]

Did John Judge and other MTA administrators not hear an outcry from an enraged electorate because the electorate simply wasn't informed about any decisions? Wide-scale public notification of the system's design happened only after contracts were signed, equipment was installed, and administrators were trying to accelerate the public's adoption of Massachusetts' "FastLane" technology. At that point it was too late to challenge the system's underlying design. Instead, consumers were simply given a "take it or leave it" choice for the convenient but admittedly invasive technology.

3. Interview with John Judge, June 27, 1997. Reported in Garfinkel, S. *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly & Associates, 2000.

## RFID Is Different

For the record, John Judge was wrong. The privacy and security considerations of RFID systems are profoundly more complex than those associated with credit cards.

For starters, radio waves are both invisible and penetrating. I cannot read your credit card if it is in your pocket, but I can read a proximity card or even an RFID-enabled credit card in that same place. Every E-ZPass or FastLane tag has a small battery that lasts for five years or so; without significantly increasing costs, each E-ZPass tag could have been equipped with a tiny speaker that would "beep" whenever the tag was read. Because it is not, there is no simple way for users of E-ZPass and the like to audit the system for themselves. Are there hidden E-ZPass readers scattered around New York City or Washington, D.C.? If each E-ZPass tag had a tiny speaker, it would be a simple matter to find out about unpublicized reader deployments.

The choice between using RFID-based payment systems on the highway and abstaining from them is profoundly different from the choice between using cash and using credit in another important way. Whether you buy your lunch with cash or a credit card, the length of the overall transaction is about the same. With RFID this is not the case. At Boston's Logan Airport on a typical weekday night, you might wait in line for 10 minutes or longer to make it through the tolls. But if you're willing to give up your privacy, you can sail through the FastLane electronic toll lane at 100 miles per hour—well, at 40 miles per hour, at least. So unlike people who buy their lunch with cash, people who try to travel the highways with cash end up paying a considerable penalty for the privilege of preserving their privacy.

It's probably too late to change a toll payment system used by Connecticut, Maine, Massachusetts, New Jersey, New York, Pennsylvania, and a growing number of other states. Today's highway regulators aren't interested in experimenting with new RFID systems; they're interested in seeing a single system deployed throughout the United States so that drivers can travel coast-to-coast without reaching for their coins. Once a technological direction is embarked upon, it is very difficult to start making incompatible choices.

This is not to say that privacy on the highway is lost. We can still have the privacy of our toll crossings; we just can't assure that privacy through technical means. But states or the federal government could pass legislation, if there were political will, to set a high threshold for protecting toll-crossing information. Such legislation could make RFID-collected toll crossing information "off limits" for use in divorce proceedings, for instance, much in the way that the Video Privacy Protection Act of 1988 (18 U.S.C. §2710) made videotape rental records

off limits. (The VPPA, better known as the Bork Bill, was passed after Judge Bork's video rental records were obtained by Washington, D.C.'s *City Paper*. The bill sped through Congress soon afterwards—allegedly because lawmakers were worried that their own video rental records might be similarly obtained and published.) RFID-protection legislation could set standards that needed to be followed for the protection of the information, and it could establish a "data retention" policy that required RFID-collected information to be destroyed after six months.

Our lawmakers could pass such legislation. All that it takes is the political will. (Stephanie Perrin and Jonathan Weinberg explore global and national privacy regulations and discuss how those regulations apply or could be applied to RFID in Chapter 4, RFID and Global Privacy Policy, and Chapter 5, RFID, Privacy, and Regulation, respectively.)

Alternatively, privacy protections can be built directly into RFID technology itself. The EPC standard, for instance, supports a "kill" command that makes it possible to permanently disable tags after they are no longer needed. If tags might be needed for some kind of post-sale use—for example, enabling a product return—it might be possible to remove the tag's antenna so that the reader needs to be in physical contact with the device. Yet another approach is the so-called RFID blocker tag that jams all RFID transmissions within a sphere around the holder—think of this as a kind of "sphere of privacy." (Ari Jules, one of the co-inventors of the blocker tag, explores these and other technological solutions to the RFID privacy problem in Chapter 21, Technological Approaches to the RFID Privacy Problem.)

## RFID Is Not Different

But on a deeper level, John Judge was right—just not for the reason that he thought. Privacy on the highways is a non-issue because the right to anonymous travel had already been considered at the dawn of the automobile and rejected.

Horses and buggies didn't have to be registered, but soon after motorized vehicles were introduced, they were required to display license plates in every state of the United States. The explicit purpose of the plates was to make every car different and, by so doing, eliminate anonymity.

These days, the technology for reading and automatically recognizing license plates has been virtually perfected. RFID-based systems are more accurate than optical license plate readers: They can read when the car is moving at a higher speed, and they are not affected by mud, rain, or fog. But

the fundamental question of anonymous travel on the roads has already been resolved in the negative: Americans don't have it—at least not if they want to drive their own cars.

And here, RFID promoters maintain, is the fundamental problem with discussing the technology in a vacuum: Practically without exception, every threat to privacy that could conceivably be caused by RFID can already be accomplished through some combination of other technologies. The cat is already out of the bag! What the RFID industry really needs to do, noted Canadian computer columnist Peter de Jager argues in Chapter 30, Experimenting on Humans Using Alien Technology, is to stop scaring the public with frightening scenarios and product names and instead clearly articulate to the public the advantage that will come from the technology—be that advantage improved customer service, lower costs, or decreased fraud.

Such thinking might be dangerous, however. Privacy activists like Beth Givens (Chapter 29, Activists: Communicating with Consumers, Speaking Truth to Policy Makers) argue that before we deploy this technology, we should more carefully assess its impact—something that really hasn't been done to date. Although it is true that stores can use store loyalty cards, credit cards, and even face-recognition technology to track people and their purchases, it may be that the increased accuracy of an RFID tag hidden in your clothing or buried in the sole of your shoe fundamentally changes the kinds of applications that stores and other businesses are willing to deploy.

## RFID and the Public's Right to Know

Whether RFID presents a doomsday scenario or not, I believe that at the very least, we have a right to know when we are being monitored by radio frequency devices. Because radio waves are invisible and penetrating, RFID has the potential to be a uniquely covert technology. I can't tell if there is an RFID tag buried in the sole of my shoe. I can't see if a store's RFID reader is silently and invisibly inventorying the clothes on my body.

Philips Semiconductors, one of the worldwide leaders in RFID, claims that it has shipped more than a billion RFID devices worldwide. This astonishing figure was announced by Mario Rivas, the company's executive vice president for communications, at the MIT RFID Privacy Workshop.

Many people in the audience were visibly shocked when Rivas made his statement. After all, RFID is usually presented in the popular press as a fledgling technology that is still being tried out, not as a mature technology that has a solid role in the worldwide marketplace. But over the past ten years, RFID has made stunning